INTERFERENCE SEARCH

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S3	0	(authentication transmission reception secret fourth first second third decider).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/08/03 13:17
S4	1	(mutual authentication information holding section acquirer generator).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/08/03 13:17
S6	1	(first device second secure area transmission reception conformity).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/08/03 13:19
S15	0	(authentication secure area first second third fourth externally).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/08/03 13:23
S16	1	(authentication secure first second third fourth externally).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/08/03 13:23

THE ACM DIGITAL LIBRARY   ⁀ Feedba

Terms used:
device and **authentication** and **secure** and **transmission** and **reception** and **first** and **second** and **third** and **fou**

Sort results by [relevance ▽]

Display results [expanded form ▽]

🔖 Save results to a Binder

❓ Search Tips

☐ Open results in a new window

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next
Best 200 shown

1 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982   Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: 📄 pdf(19.47 MB)   Additional Information: full citation, abstract, referenc

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prol
have come to rely on these systems to process and store data, we have also come to wonder a

Data security is the science and study of methods of protecting data in computer and communi

2 RFID & watermarking: Universally composable and forward-secure RFID authentication an
Tri Van Le, Mike Burmester, Breno de Medeiros
March 2007   **Proceedings of the 2nd ACM symposium on Information, computer and c**
Publisher: ACM Press
Full text available: 📄 pdf(367.90 KB)   Additional Information: full citation, abstract, referenc

Recently, a universally composable framework for RFID authentication protocols providing avail
paper we extend that framework to address forward-security issues in the presence of key com
highly practical protocols for anonymous authentication and key-exchange by RFID devices. The
random bit generator. The new protocols satisfy for ...

Keywords: RFID authentication and key-exchange protocols, anonymity, forward-security, uni

3 Fast detection of communication patterns in distributed executions
Thomas Kunz, Michiel F. H. Seuren
November 1997   **Proceedings of the 1997 conference of the Centre for Advanced Studies c**
Publisher: IBM Press
Full text available: 📄 pdf(4.21 MB)   Additional Information: full citation, abstract, referenc

Understanding distributed applications is a tedious and difficult task. Visualizations based on pr
understanding of the execution of the application. The visualization tool we use is Poet, an ever
these diagrams are often very complex and do not provide the user with the desired overview c

repeated occurrences of non-trivial commun ...

4 Computing curricula 2001

September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.63 KB) html(2.78 KB)   Additional Information: full citation, references, citings, ¡

5 Exploiting perception in high-fidelity virtual environments: Exploiting perception in high-fide
Additional presentations from the 24th course are available on the citation page
Mashhuda Glencross, Alan G. Chalmers, Ming C. Lin, Miguel A. Otaduy, Diego Gutierrez
July 2006   **ACM SIGGRAPH 2006 Courses SIGGRAPH '06**
Publisher: ACM Press
Full text available: pdf(5.07 MB) mov(68:6 MIN)   Additional Information: full citation, appendices and ¡

The objective of this course is to provide an introduction to the issues that must be considered environments. The principles of human perception guide important development of algorithms ¡ haptic rendering. We aim to show how human perception is exploited to achieve realism in high finite computational resources.In this course w ...

Keywords: collaborative environments, haptics, high-fidelity rendering, human-computer inter virtual reality

6 Essays in computing science
C. A. R. Hoare
January 1989   Book
Publisher: Prentice-Hall, Inc.
Full text available: pdf(20.91 MB)   Additional Information: full citation, abstract, referenc

Charles Antony Richard Hoare is one of the most productive and prolific computer scientists. Th There is a need, as in a Shakespearian Chorus, to offer some apology for what the book manife Selection between papers of this quality is not easy and, given the book's already considerable to be made. Pity the editor weighin ...

7 Selected writings on computing: a personal perspective
Edsger W. Dijkstra
January 1982   Book
Publisher: Springer-Verlag New York, Inc.
Additional Information: full citation, abstract, references, cited by, index terms

Since the summer of 1973, when I became a Burroughs Research Fellow, my life has been very changed: instead of going to the University each day, where I used to spend most of my time iı week and was most of the time that is, when not travelling!-- alone in my study. In my solitude more important. The circumstance that my employe ...

8 Link and channel measurement: A simple mechanism for capturing and replaying wireless
Glenn Judd, Peter Steenkiste
August 2005   **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental appro¡ WIND '05**
Publisher: ACM Press
Full text available: pdf(6.06 MB)   Additional Information: full citation, abstract, referenc

Physical layer wireless network emulation has the potential to be a powerful experimental tool. traditional simulation, is to accurately model the wireless channel. In this paper we examine thı

to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiqu
virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

9 LiSP: A lightweight security protocol for wireless sensor networks
Taejoon Park, Kang G. Shin
August 2004   **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue
Publisher: ACM Press
Full text available: pdf(487.54 KB)   Additional Information: full citation, abstract, referenc

Small low-cost sensor devices with limited resources are being used widely to build a self-orgar
situation monitoring and asset surveillance. Making such a sensor network secure is crucial to t
severe resource constraints in each sensor device. We present a *lightweight security protocol* (I
consumption via efficient rekeying. ...

Keywords: Authentication, key management, lightweight security, sensor networks

10 SPINS: security protocols for sensor netowrks
Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar
July 2001   **Proceedings of the 7th annual international conference on Mobile compu**
Publisher: ACM Press
Full text available: pdf(242.17 KB)   Additional Information: full citation, abstract, referenc

As sensor networks edge closer towards wide-spread deployment, security issues become a cer
sensor networks feasible and useful, and has not concentrated on security.

We present a suite of security building blocks optimized for resource-constrained environments
building blocks: SNEP and &mgr;TESLA SNEP provides the following important baseline security

11 Just fast keying: Key agreement in a hostile internet
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, ·
May 2004   **ACM Transactions on Information and System Security (TISSEC)**, Volume 7
Publisher: ACM Press
Full text available: pdf(324.39 KB)   Additional Information: full citation, abstract, referenc

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use in
secure; we sketch a proof of the latter property. JFK also has a number of novel engineering pa
the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-ser

Keywords: Cryptography, denial-of-service attacks

12 On randomization in sequential and distributed algorithms
Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994   **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1
Publisher: ACM Press
Full text available: pdf(8.01 MB)   Additional Information: full citation, abstract, referenc

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional del
that have been widely used in the design of randomized algorithms. These techniques are illust
distributed— that span a wide range of applications, including: primality testing (a classical prok

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dinin

isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, hashing

13 Security: Fast pre-authentication based on proactive key distribution for 802.11 infrastructi

Mohamed Kassab, Abdelfettah Belghith, Jean-Marie Bonnin, Sahbi Sassi

October 2005 **Proceedings of the 1st ACM workshop on Wireless multimedia networkin**

Publisher: ACM Press

Full text available: pdf(398.42 KB)   Additional Information: full citation, abstract, referenc

Recently, user mobility in wireless data networks is increasing because of the popularity of port applications. These applications, however, require fast handoffs among base stations to maintai handoff procedures causes a long handoff latency which affects the flow and service quality esp re-authentication latency is crucial in ord ...

Keywords: IAPP, IEEE 802.11i, WiFi, handover, pre-authentication, re-authentication

14 Distributed systems - programming and management: On remote procedure call

Patricia Gomes Soares

November 1992 **Proceedings of the 1992 conference of the Centre for Advanced Studies c**

Publisher: IBM Press

Full text available: pdf(4.52 MB)   Additional Information: full citation, abstract, referenc

The Remote Procedure Call (RPC) paradigm is reviewed. The concept is described, along with th An overview of works in supporting these mechanisms is discussed. Extensions to the paradigm studied. The main contributions of this paper are a standard view and classification of RPC mecl snapshot of the paradigm in use today and of goals for t ...

15 The relational model for database management: version 2

E. F. Codd

January 1990 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(28.61 MB)   Additional Information: full citation, abstract, referenc

From the Preface (See Front Matter for full Preface)

An important adjunct to precision is a sound theoretical foundation. The relational model is soli(logic and the theory of relations. This book, however, does not dwell on the theoretical foundati that I now perceive as important for database users, and therefore for DBMS vendors. My perce

16 Radio-layer security: Securing wireless systems via lower layer enforcements

Zang Li, Wenyuan Xu, Rob Miller, Wade Trappe

September 2006 **Proceedings of the 5th ACM workshop on Wireless security WiSe '06**

Publisher: ACM Press

Full text available: pdf(348.47 KB)   Additional Information: full citation, abstract, referenc

Although conventional cryptographic security mechanisms are essential to the overall problem (directly leverage the unique properties of the wireless domain to address security threats. The | domain-specific information that can complement and enhance traditional security mechanisms channel decorre-lates rapidly in space, tim ...

Keywords: authentication, confidentiality, fading, key establishment, propagation, wireless chi

17 VMTP: a transport protocol for the next generation of communication systems

D Cheriton
August 1986   **ACM SIGCOMM Computer Communication Review , Proceedings of the AC architectures & protocols SIGCOMM '86**, Volume 16 Issue 3
Publisher: ACM Press

Full text available: pdf(1.40 MB)   Additional Information: full citation, abstract, referenc

The Versatile Message Transaction Protocol (VMTP) is a transport-level protocol designed to sur communication. The protocol is optimized for efficient page-level network file access in particule VMTP design, including the VMTP treatment of sessions, addressing, duplicate suppression, flow multicast. The VMTP design refle ...

18 Key management and key exchange: Efficient, DoS-resistant, secure key exchange for int

William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, Angelo:
November 2002   **Proceedings of the 9th ACM conference on Computer and communication**
Publisher: ACM Press

Full text available: pdf(118.52 KB)   Additional Information: full citation, abstract, referenc

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Ar proof of the latter property. JFK also has a number of novel engineering parameters that permit the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: cryptography, denial of service attacks

19 Security: Enhancing the security of corporate Wi-Fi networks using DAIR

Paramvir Bahl, Ranveer Chandra, Jitendra Padhye, Lenin Ravindranath, Manpreet Singh, Alec Wolr
June 2006   **Proceedings of the 4th international conference on Mobile systems, appli**
Publisher: ACM Press

Full text available: pdf(302.26 KB)   Additional Information: full citation, abstract, referenc

We present a framework for monitoring enterprise wireless networks using desktop infrastructu *Array of Inexpensive Radios*. We demonstrate that the DAIR framework is useful for detecting r corporate networks, as well as for detecting Denial of Service attacks on Wi-Fi networks.Prior p combination of access points (APs), m ...

Keywords: 802.11, denial-of-service, rogue AP, security, wireless networks

20 Wireless monitoring and denial of service: Channel surfing and spatial retreats: defenses a

Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang
October 2004   **Proceedings of the 2004 ACM workshop on Wireless security WiSe '04**
Publisher: ACM Press

Full text available: pdf(327.10 KB)   Additional Information: full citation, abstract, referenc

Wireless networks are built upon a shared medium that makes it easy for adversaries to launch service is targeted at preventing sources from communicating. These attacks can be easily accc protocols, or emitting a radio signal targeted at jamming a particular channel. In this paper we devices to evade a MAC/PHY-layer jamming-style wi ...

Keywords: CSMA, Jamming, denial of service

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	422	(713/169).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/08/03 12:52
S2	297	S1 and @ad<"20020708"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/03 13:04
S3	104	(MINEMURA and ATSUSHI).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/03 13:05
S5	13	authenication and concat$8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/03 13:07
S6	17	authenicat$3 and concat$8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/03 13:08
S9	659	((cell or cellular or mobile) adj (telephone or phone)) same authenticat$4 same ((memory adj (card or device)) or (smart adj card) or smartcard or smart?card)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/03 13:10

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	641	((cell or cellular or mobile) adj (telephone or phone)) same authenticat$4 same ((memory adj (card or device)) or (smart adj card) or smartcard or smart?card)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 21:09
S2	196	S1 and @ad<"20020708"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 21:10
S3	54	S2 and ((random adj number) or RAND)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 19:55
S4	16	S3 and (serial adj number)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 19:56
S5	10	S4 and (pin or userid or (user adj (info or information or id or identification)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 19:57
S6	1020	((cell or cellular or mobile) adj (telephone or phone)) same authenticat$4 same ((memory adj (card or device)) or (smart adj card) or smartcard or smart?card or SIM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:52
S7	278	S6 and @ad<"20020708"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 21:56
S8	2	("5241598").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/07/08 21:12
S9	14	S7 and (encrypt$ same PIN same key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 21:57

S10	666	713/169	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:01
S11	107	S10 and concat$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:02
S12	81	S11 and @ad<"20020708"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:46
S13	23	S12 and (smart adj card)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:44
S14	58	generat$3 same pin same concat$9 same (secret or serial)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:46
S15	35	generat$3 same pin same concat$9 same (secret or serial) same compar$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:46
S16	31	S15 and @ad<"20020708"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:53
S17	1034	((cell or cellular or mobile) adj (telephone or phone)) same authenticat$4 same ((memory adj (card or device)) or (smart adj card) or smartcard or smart?card or SIM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:52
S19	86	S17 and concat$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:52

EAST Search History

S20	16	S19 and @ad<"20020708"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:53